IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

HILARY REMIJAS, MELISSA FRANK, DEBBIE FARNOUSH, and JOANNE KAO, individually and on behalf of all others similarly situated, Plaintiffs, v. THE NEIMAN MARCUS GROUP, LLC, a Delaware limited liability company, Defendant.	Case No. 1:14-cv-01735 Hon. James B. Zagel Magistrate Judge Maria Valdez

PLAINTIFFS' RESPONSE IN OPPOSITION TO NEIMAN MARCUS GROUP, LLC'S SUPPLEMENTAL BRIEF IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT CASES

UNITED STATES COURT OF APPEALS CASES

UNITED STATES DISTRICT COURT CASES

STATE SUPREME COURT CASES

STATE COURT OF APPEALS CASES

STATE STATUTES & RULES

I. INTRODUCTION

The Seventh Circuit held that Defendant's motion to dismiss for lack of standing fails, and so too does its motion to dismiss for failure to state a claim. Defendant could and should have avoided the data breach that affected its stores in 2013, and Defendant is liable for its failure to do so, which directly injured the named Plaintiffs in this action, under statutory law including the state data breach acts and consumer protection laws invoked in the First Amended Complaint (Dkt. 27, "FAC"), and under the common law theories advanced.

On appeal from this Court's prior dismissal of this action, the Seventh Circuit held that Plaintiffs suffered real, concrete injuries which give them standing under Article III of the U.S. Constitution, including "costs associated with the process of sorting things out" after the data breach (Dkt. 66 (hereinafter the "Opinion") at 7), as well as "'the risk that Plaintiffs' personal data will be misused by the hackers'" in the future (*id.* at 8 (quoting *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)). Defendant's supplemental brief ignores on-point authority, cited by the Seventh Circuit itself, under which the same allegations that give Plaintiffs' Article III standing also support Plaintiffs' claims under California's Customer Records Act ("CRA") for Defendant's failure to implement "reasonable security." Cal. Civ. Code 1798.81.5; *Adobe*, 66 F. Supp. 3d at 1218 (reasoning that "Plaintiffs' allegations of injury-in-fact satisfy the CRA's statutory standing requirement for the same reasons these allegations satisfy Article III," and denying Adobe's "Motion to Dismiss Plaintiffs' CRA claim for violations of Section 1798.81.5").

Defendant's failures to implement and maintain reasonable security procedures that could have prevented the data breach include its inexplicable decisions to "turn[] off" security systems that would have blocked the hackers' efforts, and to ignore some 59,746 alerts on its system

regarding "suspicious behavior." (FAC ¶36.)[1] As a consequence, the hackers were able to remain in Defendant's system—undetected—for over ten months, and to steal the payment card data ("PCD") and personally identifiable information ("PII") (collectively, "Private Information") of at least 350,000 consumers. Defendant admits that at least "approximately 9,200 [credit or debit cards used at its stores] were subsequently used fraudulently elsewhere." (*Id.* ¶¶41-42.)

In its supplemental briefing, Defendant mischaracterizes or ignores allegations demonstrating that Plaintiffs were directly harmed by Defendant's failure to issue prompt notification of the data breach after its credit card processor informed Defendant "that fraudulent card usage had been linked to a 'common point of purchase'" at Defendant's stores on December 13, 2013. (*Id*. ¶28.) Plaintiffs Kao and Remijas allege that they made purchases at Defendant's stores in the following days and weeks—during the busy holiday shopping season that Defendant did not want to compromise for fear of injuring its bottom line, never mind injuries that its consumers might suffer by virtue of continued fraud resulting from the data breach—which they would not have made had they known about the data breach. (*Id*. ¶¶3, 6.)

Not only do such allegations support Plaintiffs' claims under state data breach laws, but they also support Plaintiffs' claims under the consumer protection laws of all 50 states, which Defendant barely addresses other than to assert, without any basis, that Plaintiffs somehow fail to allege "actual injury" despite the Seventh Circuit's Opinion, which clearly supports the contrary conclusion. Plaintiffs have included with this supplemental opposition an Appendix of state consumer protection laws that describes each state's law and how Plaintiffs' allegations satisfy its

[1] Plaintiffs summarized the FAC's factual allegations in Part II of their original opposition, and will not repeat that summary in this supplemental brief. (Dkt. 39.) Rather, the most pertinent allegations are referenced in this Introduction and in the appropriate sections of the Argument, *infra*.

requirements.

With respect to California's Unfair Competition Law ("UCL"), in particular, *Adobe* is on-point and, again, un-cited by Defendant in its supplemental brief despite the Seventh Circuit's heavy reliance on the decision's reasoning and its particular force with respect to California law. The *Adobe* court correctly reasoned the "alleged CRA violation is sufficient to sustain Plaintiffs' UCL unlawful claim." *Adobe*, 66 F. Supp. 3d at 1226. There is no reason for this Court to reach a different conclusion here.

Defendant's negligent behavior, combined with the injuries to Plaintiffs that the Seventh Circuit held support Article III standing, fully support Plaintiffs' claims for negligence, breach of implied contract, invasion of privacy, and unjust enrichment. The theft of Plaintiffs' and other class members' Private Information, which they entrusted to Defendant, has resulted in actual injuries including fraudulent charges and phishing directed at the named Plaintiffs. The theft also significantly increases the risk that Plaintiffs and other class members will suffer identity theft in the future, as recognized by the Seventh Circuit.

Defendant neither adequately warned Plaintiffs and other class members about the true consequences of the theft of their Private Information, nor has it sufficiently compensated them for the harm caused by its failure to implement reasonable data security measures. Defendant's motion to dismiss should be denied.

II. THE SEVENTH CIRCUIT'S RULING

In its Opinion, the Seventh Circuit held that Plaintiffs' allegations establish Article III standing. In particular, the panel held that:

> the 9,200 [customers] who already have incurred fraudulent charges have experienced harm. Those victims have suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges. The complaint also alleges a concrete risk of harm for the rest [of the class members].

(Opinion at 6-7.)

The court reasoned that "there are identifiable costs associated with the process of sorting things out" when fraudulent charges are made to a victim's payment card. (*Id.* at 7.) The court recognized that Defendant's position that all fraudulent charges are reimbursed by banks 100% of the time "reveals a material factual dispute[2] on such matters as the class members' experiences and both the content of, and the universality of, bank reimbursement policies." (*Id.* at 7-8.)

The Seventh Circuit quoted at length from the district court opinion in *Adobe*, which denied a motion to dismiss similar to that presently before the Court in this action. "Like the *Adobe* plaintiffs," reasoned the Seventh Circuit, "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur." (*Id.* at 9 (quoting *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013)). The Seventh Circuit recognized that "'the risk that Plaintiffs' personal data will be misused by the hackers who breached [Defendant]'s network is immediate and very real.'" (Opinion at 8 (quoting *Adobe*, 66 F. Supp. 3d at 1214).)

> Requiring the plaintiffs "to wait for the threatened harm to materialize in order to sue" would create a different problem: "the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach."
>
> . . . .
>
> At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.

(*Id.* at 9 (quoting *Adobe*, 66 F. Supp. 3d at n.5.).) In addition to the risk of future injury, the

[2] In its supplemental brief, Defendant does not appear to rely on banks' "zero liability" in support of its motion to dismiss. Insofar as Defendant continues to rely on these policies, which Defendant invoked in its original motion, the Seventh Circuit's Opinion clearly states these are factual issues not appropriate for decision on a motion to dismiss.

Seventh Circuit held that Plaintiffs' actual injuries, including "lost time and money protecting themselves against future identity theft and fraudulent charges," supported Article III standing. (Opinion at 10.) The cost of credit monitoring "easily qualifies as a concrete injury." (*Id.* at 11.)

The Seventh Circuit did "not decide whether" Plaintiffs' other asserted injuries supported standing under Article III. (*Id.*) Defendant wrongly suggests that the Seventh Circuit somehow rejected Plaintiffs' "Overpayment Theory." (Supp. Br. at 4-5.) However, the court did no such thing—rather, the Seventh Circuit "refrain[ed] from deciding whether the overpayment for Neiman Marcus products and the right to one's personal information might suffice as injuries under Article III. The injuries associated with resolving fraudulent charges and protecting oneself against future identity theft do." (Opinion at 14.)

The panel reasoned that, "[i]n some situations, we have held that financial injury in the form of an overcharge can support Article III standing," and that "District courts have applied this approach to comparable situations." (*Id.* at 11-12 (citing *In re Aqua Dots Products Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011); *Chi. Faucet Shoppe, Inc. v. Nestle Waters N. Am. Inc.*, No. 12 C 08119, 2014 WL 541644, at *3 (N.D. Ill. Feb. 11, 2014) (citing *Aqua Dots*); *Muir v. Playtex Products, LLC*, 983 F. Supp. 2d 980, 986 (N.D. Ill. 2013) (holding that a claim that consumer would not have purchased product or not have paid a premium price for the product is sufficient injury to establish standing).) The court recognized that applying the same reasoning in this case "would extend that idea from a particular product to the operation of the entire store," but did not answer the question of how the Seventh Circuit would come down on the issue, instead concluding: "This is a step that we need not, and do not, take in this case." (Opinion at 12.) The court clearly understood the logic of Plaintiffs' theory, and recognized that it finds support in cases such as *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012) (cited in Opinion at 12) (reasoning

plaintiff suffered financial injury from paying higher premiums in light of defendant's failure to implement security policies).

With regard to the requirement that the injury-in-fact supporting standing be caused by Defendant's conduct, the Seventh Circuit reasoned: "It is certainly plausible for pleading purposes that [Plaintiffs'] injuries are 'fairly traceable' to the data breach at Neiman Marcus." (Opinion at 15 (quoting *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) ("Plaintiffs' allegations plausibly allege that they suffered injuries that are 'fairly traceable' to Target's conduct. This is sufficient at this stage to plead standing. Should discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment on the issue.")).)

Defendant urged the Seventh Circuit to affirm this Court's dismissal under Rule 12(b)(6) as well as on standing grounds, but the panel refused to do so and chided Defendant for failing to file any cross-appeal regarding the 12(b)(6) aspect of its original motion and this Court's original ruling on it. (Opinion at 16-17.)

III. ARGUMENT

Plaintiffs described the applicable standard for a 12(b)(6) motion in their original opposition, and will not repeat it here. Suffice it to say that Plaintiffs' FAC survives Defendant's motion because it alleges "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

A. The California Plaintiffs Plead Violation of State Data Breach Acts (Count VI)

Plaintiffs' sixth cause of action alleges that Defendant violated 14 states' data breach acts. Defendant's argument in its supplemental brief focuses almost entirely on California's act, the CRA, Cal. Civ. Code §§ 1798.80, *et seq.* Defendant wrongly argues that Plaintiffs fail to allege a cognizable injury (Supp. Br. at 22), citing that section of the CRA which states: "Any customer injured by a violation of this title may institute a civil action to recover damages." Cal. Civ. Code

§ 1798.84(b).

1. Plaintiffs State a Claim Under Section 1798.81.5(b) of the CRA

As Judge Koh reasoned in *Adobe*: "Although Section 1798.84 does not define what qualifies as an injury under the statute, other courts in the Ninth Circuit have found that an injury that satisfies Article III's injury-in-fact standard suffices to establish statutory injury under the CRA." *Adobe*, 66 F. Supp. 3d at 1218. The *Adobe* court held "that Plaintiffs' allegations of injury-in-fact satisfy the CRA's statutory standing requirement for the same reasons these allegations satisfy Article III," and denied Adobe's "Motion to Dismiss Plaintiffs' CRA claim for violations of Section 1798.81.5." *Id.*

Section 1798.81.5 of the CRA—which supported the claim that survived a motion to dismiss in *Adobe* that was similar to Defendant's motion here—requires Defendant "to provide reasonable security" for the Private Information of Californians. Cal. Civ. Code § 1798.81.5(a)(1). Defendant never really addresses this claim in its original brief or in its supplemental brief.

Plaintiffs allege that Defendant "turned off" its "system's ability to automatically block" the malware used in the data breach (FAC ¶36), and failed to segregate its customers' PCD and PII (*id.* ¶35). Defendant can hardly contend that such deficient security is the "reasonable security" required by the CRA, which consumers expect. Cal. Civ. Code § 1798.81.5. Just as in *Adobe*, Plaintiffs here state a claim under the CRA. As Plaintiffs argued in their original opposition, they adequately allege a claim for violation of § 1798.81.5. (Dkt. No. 39 at 21-22 (citing, *inter alia*, FAC ¶¶5, 6, 13-14, 28-40, 53, 54, 136, 138(a), 139, 145, 146).)

Plaintiffs seek damages for Defendant's CRA violations under Cal. Civ. Code § 1798.84(b), which allows "[a]ny customer injured by a violation of this title" to "institute a civil action to recover damages." *Id.* And Plaintiffs are entitled to injunctive relief under Cal. Civ. Code § 1798.84(e), which provides that "[a]ny business that violates . . . this title may be enjoined."

Other courts have recognized that allegations similar to Plaintiffs' are sufficient to state a claim under the CRA and under California's UCL. *See In re Sony Gaming Networks and Customer Data Breach Sec. Litig*. ("*Sony II*"), 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) (denying motion to dismiss claim for injunctive relief under CRA); *Adobe*, 66 F. Supp. 3d at 1218, 1225-26 (denying motion to dismiss claims under CRA and UCL based on alleged failure to implement reasonable security measures).[3] Defendant's motion to dismiss Plaintiffs' CRA claim should be denied because Plaintiffs' allegations clearly establish that Defendant failed to implement reasonable cyber security.

2. Plaintiffs State a Claim Under Section 1798.82 of the CRA and the Other State Data Breach Acts Invoked, All of Which Require Prompt Notification

Plaintiffs' allegations also state a claim under those provisions of the CRA requiring Defendant to issue prompt and full notice of the data breach to affected consumers—a requirement similarly imposed by the other state data breach acts cited in Paragraph 138 of the FAC. Defendant attempts to parlay that portion of the Opinion stating that, under "California law, a delay in notification is not a cognizable injury," from an argument about federal standing into an argument about what constitutes a substantive violation of these states' statutory laws. (Opinion at 13 (citing *Price v. Starbucks Corp.*, 192 Cal. App. 4th 1136, 1143 (Cal. Ct. App. 2011)).)

First, Plaintiffs allege more than a delay in notification. Defendant failed to provide Plaintiff Remijas with any notice of the data breach whatsoever. (FAC ¶3.) Other Plaintiffs received inadequate notices that failed to include information required by the CRA, including dates. (*Id*. ¶¶4, 6, 48, 56)

[3] Plaintiffs' claims in this case are even stronger than the *Adobe* plaintiffs' claims, given the allegations that many named Plaintiffs and class members have suffered identity theft and fraudulent charges on their cards as a direct result of Defendant's data breach.

Second, as argued in Plaintiffs' original opposition (Part IV. B. at 2-3), Plaintiffs allege that they were harmed by Defendant's delay in issuing, and/or failure to issue, the required notifications. In its supplemental brief, Defendant dismisses Plaintiff Kao's allegations that she was injured directly by Defendant's delay in notification as "another instance of the invalid Overpayment Theory." (Supp. Br. at 24.) Not only is the "Overpayment Theory" not "invalid," as discussed above,[4] but this characterization of Plaintiff Kao's allegations simply is not correct. She alleges that she used a credit card to make a purchase at Defendant's stores on December 31, 2013—during that period of the holiday shopping season when Defendant knew about the data breach but chose not to issue any notification. (FAC ¶4.) Had Defendant provided notice in the most "expedient time possible and without unreasonable delay," Plaintiff Kao could have avoided using her credit card at Defendant's store on that day, and her information would not have been compromised.[5] Plaintiff Kao suffered economic injury as a consequence of Defendant's untimely notice because she spent money on December 31, 2013 to purchase a product she would not have otherwise purchased. *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 316-17 (Cal. 2011); *see also Hinojos v. Kohl's Corp.*, 718 F.3d 1098, 1107 (9th Cir. 2013).

Defendant is similarly wrong to scorn Plaintiff Remijas' allegations of injury flowing from delayed notification. Defendant's argument in its supplemental brief that Plaintiffs are precluded from pursuing a claim under the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.* (the "PIPA"), because they fail to allege "actual damages" (Supp. Br. at 24-25) ignores the

---

[4] *See supra* Part II.

[5] In a footnote, Defendant argues that Plaintiff Kao's card could not have been compromised on December 31, 2013, because the malware "did not operate after October 30, 2013," (Supp. Br. at n.9), but Plaintiffs plausibly allege that "[i]t's very unusual for malware to self-expire" in the manner Defendant claims here, and Plaintiffs allege that the data breach was not contained until January 10, 2014. (FAC ¶¶34, 40.) Defendant's argument in this regard raises issues of fact not amenable to resolution on the present motion to dismiss.

FAC's allegations, which must be accepted as true at this stage of the litigation. Plaintiffs allege that Defendant first learned about the data breach on December 13, 2013, when its credit card processor informed Defendant "that fraudulent card usage had been linked to a 'common point of purchase'" at Defendant's stores. (FAC ¶28.) Plaintiff Remijas, an Illinois resident, made a purchase at Defendant's store on December 21, 2013, which could have been avoided if Defendant had complied with its obligation to provide prompt notification of the data breach, as required by the PIPA and the other state data breach acts invoked in the FAC. (FAC ¶3.) Accordingly, Plaintiff Remijas suffered actual damages—the same types of damages identified by the Seventh Circuit including "costs associated with the process of sorting things out" (Opinion at 7)—that were caused by Defendant's delay in notification and its violation of its statutory duties under the PIPA and other state data breach acts.

Finally, even if Plaintiffs were precluded from pursuing monetary damages under the CRA and other state data breach acts—damages to which Plaintiffs are entitled in light of their allegations that they suffered harm as a result of Defendant's delay in issuing, or failure to issue, the required notifications—Plaintiffs nonetheless would be entitled to pursue injunctive relief under these statutes. *See Sony*, 996 F. Supp. 2d at 1010 (denying motion to dismiss and reasoning that "Plaintiffs may pursue their injunctive relief claims under § 1798.84(e), which affords relief when a 'business violates, proposes to violate, or has violated' the [CRA]'"). Defendant's motion to dismiss should be denied.

B. Plaintiffs State a Claim Under State Consumer Protection Laws (Count IV)

Plaintiffs allege facts showing that Defendant violated the consumer protection laws cited in Count IV of the FAC in several ways. Defendant violated these statutes through its:

(1) Failure to maintain adequate computer systems and data security practices to safeguard its customers' Private Information (*see* FAC ¶¶ 35-36, 39, 107-08);

(2) Failure to disclose that its computer systems and data security practices were inadequate to safeguard Private Information (*see id*.);

(3) Failure to timely and accurately disclose the data breach to Plaintiffs (*id*., ¶¶ 28-31, 120, 125); and

(4) Continued acceptance of card payments, failure to segregate PCD and PII, and unsafe storage of Private Information after Defendant's security vulnerabilities and the data breach were, or should have been, known to Defendant (*id*., ¶¶ 28-29, 33-34, 120, 125).

Plaintiffs have stated claims based on one or more of these theories for each consumer protection statute alleged in the Complaint. *See* Plaintiffs' Appendix: Overview of State Consumer Protection Laws (setting forth violations of statutes and cross-referencing Plaintiffs' allegations).

With respect to California's UCL, in particular, *Adobe* is on-point and, again, un-cited by Defendant in its supplemental brief despite the Seventh Circuit's heavy reliance on the decision's reasoning and its particular force with respect to California law. The *Adobe* court correctly reasoned the "alleged CRA violation is sufficient to sustain Plaintiffs' UCL unlawful claim." *Adobe*, 66 F. Supp. 3d at 1226. There is no reason for this Court to reach a different conclusion.

The *Adobe* court also held that plaintiffs' allegations supported a claim under the UCL's "unfair" prong, because they "allege[d] that Adobe's conduct placed Plaintiffs at a substantial risk of future harm and caused Plaintiffs to overpay for Adobe products and services." *Id.* at 1227. Like the "Overpayment Theory" Defendant wrongly dismisses in this case, the *Adobe* court accepted allegations that plaintiffs there "allege[d] they personally spent more on Adobe products than they would had they known Adobe was not providing the reasonable security Adobe represented it was providing," in order to find not only standing, but that plaintiffs stated a claim

under California's UCL. *Id.* at 1224.

Adobe underscores the reasoning and argument set forth in Part IV. D. 2 of Plaintiffs' original opposition, which will not be repeated here. Again, Defendant argues Plaintiffs have not suffered a cognizable injury under the UCL as well as under New York and Illinois law. (*See* MTD at 6-18, 19-22, 30; Supp. Br. at 20-21.) For all the reasons set forth in Plaintiffs' original opposition, Defendant continues to be wrong. The same injuries that the Seventh Circuit relied upon to conclude that Plaintiffs have standing support Plaintiffs' claims under consumer protection laws.

C. Plaintiffs Properly Plead Breach of Implied Contract (Count II)

Defendant's supplemental brief adds little to the argument made in the original motion to dismiss concerning Plaintiffs' claim for breach of implied contract, except again to misconstrue the Seventh Circuit's opinion as rejecting Plaintiffs' "Overpayment Theory." As discussed *supra* Part II, the Seventh Circuit in no respect rejected Plaintiff's allegations that they paid a price premium that should have been used to protect Plaintiffs' PII through adequate security measures (that were not implemented and in fact were turned off). (FAC ¶16.) Rather, the Seventh Circuit "refrain[ed] from deciding whether the overpayment for Neiman Marcus products and the right to one's personal information might suffice as injuries under Article III. The injuries associated with resolving fraudulent charges and protecting oneself against future identity theft do." (Opinion at 14.)

The Seventh Circuit cited and followed prior data breach opinions that approved of this theory. *AvMed* in particular found that such allegations specifically support a claim for breach of implied contract in a data breach case. *AvMed*, 693 F.3d at 1328 (finding plaintiffs sufficiently pled breach of implied contract in data breach case where they alleged "that AvMed cannot equitably retain their monthly insurance premiums—part of which were intended to pay for the

administrative costs of data security—because AvMed did not properly secure Plaintiffs' data . . ."); *see also Adobe*, 66 F. Supp. 3d at 1224 (finding plaintiffs stated claim under UCL where they "allege[d] they personally spent more on Adobe products than they would had they known Adobe was not providing the reasonable security Adobe represented it was providing").

Here, Plaintiffs allege that "[c]onsumers place value in data privacy and security, and they consider it when making purchasing decisions." (FAC ¶15.) Plaintiffs allege they would not have made their purchases at Defendant's store had they known that Defendant failed to implement reasonable data security. (*Id.*) Plaintiffs allege the existence of "an implied contract with Defendant that Defendant will adequately secure and protect their Private Information, and will use part of the purchase price of the goods to pay for adequate data security measures." (*Id*. ¶16.) Plaintiffs further allege that Defendant failed to implement such adequate data security measures, instead turning off systems that would have prevented the data breach and ignoring nearly 60,000 alerts concerning it. (*Id*. ¶36.) As a result, Plaintiffs were harmed—at the very least, in the amount of the price premium attributable to adequate data security, but also in various other ways alleged in the FAC, including by incurring fraudulent charges and by receiving phishing phone calls. (*Id*. ¶¶44-57.)

Plaintiffs stand by the argument advanced in their original opposition, and properly state a claim for breach of implied contract.

D. <u>Plaintiffs State a Claim for Negligence (Count I)</u>

1. Plaintiffs Allege a Cognizable Injury

As argued in Plaintiffs' original opposition, they plausibly allege every required element of a negligence claim. (Dkt. 39, Part IV. F. 1.) Defendant focuses on the injury element in its supplemental briefing, *inter alia* repeating the argument made in its original motion that relies on *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007), to assert Plaintiffs suffered no

cognizable injury supporting a negligence claim here. (Supp. Br. at 11.) But as argued in Plaintiffs' original opposition, Plaintiffs' alleged actual damages including unauthorized charges and phishing, in addition to their allegations concerning the price premium they paid for reasonable data security measures that were not implemented, distinguish this case from *Pisciotta*.

Plaintiffs allege that Defendant's negligence included turning off a system that would have prevented the data breach from occurring and ignoring approximately 60,000 alerts concerning the data breach. (FAC ¶36.) Plaintiffs further allege that they actually incurred fraudulent charges on their cards and that Plaintiff Frank received a frightening "phishing" call on her personal cell phone, all as a result of the data breach and Defendant's negligence. (FAC ¶¶44-58.) The *Pisciotta* case did not consider comparable allegations. 499 F.3d at 632.

Defendant argues that "[n]o court, including the panel in this matter, has recognized a reimbursed unauthorized charge, standing alone, as a sufficient injury for the purpose of conferring Article III standing, let alone as injury sufficient to state a claim for negligence." (Supp. Br. at 14.) But here Defendants conveniently overlook the panel's observations: (a) "that full reimbursement is not guaranteed"; (b) that despite reimbursement consumers are injured because such "victims have suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges"; and (c) that such argument "reveals a ***material factual dispute*** on such matters as the class members' experiences and both the content of, and the universality of, bank reimbursement policies" that cannot be resolved on a motion to dismiss. (Opinion at 7-8 (emphasis added).)

In its supplemental briefing regarding the injury element of Plaintiffs' negligence claim, Defendant again argues that the Seventh Circuit supposedly rejected Plaintiffs' "Overpayment

Theory," but that is not true. As mentioned above, the panel cited *AvMed* (*id.* at 12), a case in which the Eleventh Circuit validated this very theory:

> Plaintiffs allege that they conferred a monetary benefit on AvMed in the form of monthly premiums, . . . that AvMed uses the premiums to "pay for the administrative costs of data management and security," and that AvMed "should not be permitted to retain the money belonging to Plaintiffs . . . because [AvMed] failed to implement the data management and security measures that are mandated by industry standards." Plaintiffs also allege that AvMed either failed to implement or inadequately implemented policies to secure sensitive information, as can be seen from the data breach. Accepting these allegations as true, we find that Plaintiffs alleged sufficient facts to allow this claim to survive a motion to dismiss.

AvMed, 693 F.3d at 1328.

AvMed concerned a data breach in which two computers were stolen from Defendant's offices, which contained customers' Private Information. The court in *AvMed* found

> that the complaint states a cognizable injury for the purposes of standing . . . . We also conclude that the Complaint sufficiently alleges the causation element of negligence, negligence per se, breach of contract, breach of implied contract, breach of the implied covenant of good faith and fair dealing, and breach of fiduciary duty . . . . The Complaint similarly alleges facts sufficient to withstand a motion to dismiss on the restitution/unjust enrichment claim.

Id. at 1321.

The *AvMed* court denied a 12(b)(6) motion to dismiss and rejected defendant's arguments that plaintiffs must plead "'unreimbursed losses'" in addition to ordinary "'losses,'" finding that plaintiffs' allegations that they suffered "financial injury" sufficed because "monetary loss is cognizable under Florida law for damages in contract, quasi-contract, negligence, and breach of fiduciary duty." *Id.* at 1324. "In this digital age, our personal information is increasingly becoming susceptible to attack. People with nefarious interests are taking advantage of the plethora of opportunities to gain access to our private information and use it in ways that cause real harm." *Id.* at 1329.

Defendants cannot demonstrate that bank reimbursement policies fully remedied any injury

in this action, with regard to Plaintiffs' negligence claim or otherwise. Plaintiffs allege injuries that support their negligence claim as well as the other claims advanced.

2. The Economic Loss Rule Does Not Bar Plaintiffs' Negligence Claims

Plaintiffs contend that cases applying the economic loss rule to bar analogous negligence claims in California (*Sony*)[6] and Illinois (*In re Michaels Stores Pin Pad Litig.*)[7] were wrongly

[6] The California Supreme Court has employed a six-factor "special relationship" analysis to determine whether a plaintiff may recover purely economic loss in claims for negligent performance of services. *See J'Aire Corp. v. Gregory*, 598 P.2d 60, 62-63 (Cal. 1979) (finding "special relationship" precluding application of economic loss rule). The factors considered include: (1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct and (6) the policy of preventing future harm. *Id.* at 63. All six factors must be considered by the court and the presence or absence of one factor is not decisive. *See Kalitta Air, LLC v. Cent. Tex. Airborne Sys., Inc.*, 315 Fed. Appx. 603, 605-06 (9th Cir. 2008).

Each *J'Aire* factor is satisfied here. Plaintiffs' allegations show that they had a "special relationship" with Defendant (FAC ¶¶28-31, 33-36, 39, 107-08, 120, 125) and that: (1) Plaintiffs would not have shopped at Defendant's stores had they known of its data security practices (*id*. ¶¶15, 69, 89); (2) the harm was foreseeable (*id*. ¶¶17-20, 114); (3) Plaintiffs suffered a variety of injuries (*id*. ¶¶45-47, 51, 53, 55); (4) Plaintiffs' injuries flowed directly from the breach (*id*. ¶87, 90); (5) the degree of negligence is severe and there is a strong moral blame attached to Defendant's reckless conduct (*id*. ¶93); and (6) there is a strong public policy to protect customers personal and financial information (*id*. ¶¶15-20).

[7] Illinois law recognizes three exceptions to the economic loss rule: (1) where plaintiff sustains personal injury or property damage resulting from a sudden or dangerous occurrence; (2) where plaintiff's damages were proximately caused by defendant's intentional, false representation; and (3) where plaintiff's damages were proximately caused by the negligent misrepresentation of a defendant in the business of supplying information for the guidance of others in business transactions. *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011). Plaintiffs satisfy each of these exceptions in that the fraud they experienced happened without warning after the data breach and they continue to be threatened by it; Defendant concealed its inadequate data security before the data breach and initially concealed the data breach after learning of its occurrence; and Defendant ignored over 60,000 malware alerts that could have prevented or mitigated the data breach.

In re Michaels is distinguishable because the court did not apply relevant exceptions. *See* 830 F. Supp. 2d. at 530 ("Plaintiffs do not argue that they satisfy any of the three exceptions set forth in *Moorman*. Rather, Plaintiffs argue that the economic loss rule does not apply"). The *Target* court followed *In re Michaels* on this point without applying the economic loss rule exceptions to the facts in that case. *See In re Target Corp. Customer Data Sec. Breach Litig.*, 66

decided.

With respect to the law of New York, however, Defendants again ignore on-point authority which the Seventh Circuit cited in its Opinion: *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154 (D. Minn. 2014) (cited in Opinion at 15). Although the *Target* court dismissed plaintiffs' negligence claims through application of the economic loss rule under the laws of several states, it refused to do so with respect to New York. The *Target* court reasoned that because plaintiffs alleged "a quasi-contractual, privity-like relationship with respect to their personal financial information," New York's "independent-duty exception to the economic loss rule" applied and "[d]ismissal of Plaintiffs' New York negligence claims is not appropriate." *Id.* at 1175 (citing *In re Facebook Inc., IPO Sec. & Derivative Litig.*, 986 F. Supp. 2d 428 (S.D.N.Y. 2013)); *see also Rochester-Genesee Reg'l Trans. Auth. V. Cummins Inc.*, No. 09-CV-6370-MAT, 2010 WL 2998768, at *8 (W.D.N.Y. July 28, 2010) ("[U]nder New York law, a Plaintiff may bring a cause of negligence where a legal duty independent of contractual obligations has been breached."); *Hydro Investors, Inc. v. Trafalgar Power Inc.*, 227 F.3d 8, 16 (2d Cir. 2000).

In its supplemental brief, Defendant primarily relies upon *King County v. IKB Deutsche Industriebank AG*, 863 F. Supp. 2d 288 (S.D.N.Y. 2012), in support of its argument that New York's economic loss rule should apply here. That was not a data breach case. Furthermore, the *King County* court recognized the independent-duty exception that the *Target* court applied, reasoning however that the banks and ratings agencies at issue there did not owe such a duty toward the institutional investors plaintiffs in that securities case. *King County*, 863 F. Supp. 2d at 303. That reasoning is inapplicable to this data breach case, where the *Target* court's reasoning applies

F. Supp. 3d 1154, 1174 (D. Minn. 2014). Here, Plaintiffs contend that the *Moorman* exceptions apply, an issue that never was considered in *In re Michaels* or in *Target*.

with full force.

Defendant also continues to rely upon *Hammond v. Bank of N.Y. Mellon Corp.*, 08 Civ. 6060, 2010 WL 2643307 (S.D.N.Y. June 25, 2010) (cited in MTD at 19; Supp. Br. at 15), but as argued in Plaintiffs' original opposition, *Hammond* did not interpret or apply the economic loss rule at all. Rather, the court in that case dismissed the negligence claims after finding that: (1) the defendant bank, which had no "direct dealings" with plaintiffs whatsoever, owed no duty to plaintiffs; and (2) plaintiffs alleged injuries, which consisted solely of "heightened fear of having their identities stolen in the future," were inadequate because they lacked "a 'high degree of probability that a future injury will occur.'" *Id.* at *9-10 (quoting *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 281 (S.D.N.Y. 2008)). Plaintiffs' allegations of actual injury in this case—which the Seventh Circuit accepted in its Opinion—distinguish *Hammond*, in that they not only demonstrate a "high degree of probability" of future injury, but an actual, present injury as well.[8] *Id.*

3. Plaintiffs Plausibly Allege Causation for Purposes of Their Negligence Claim, and All Other Claims

In its supplemental briefing attacking Plaintiffs' negligence claim, Defendant again argues that Plaintiffs somehow fail to allege causation. (Supp. Br. at 17-18.) Defendant argues that causation for purposes of a negligence claim is more demanding than for purposes of the standing analysis performed by the Seventh Circuit, but Defendant fails to apply any of this reasoning to the facts alleged, not even referencing Plaintiffs Remijas and Kao's factual scenarios.

[8] These allegations also distinguish *Caudle*, 580 F. Supp. 2d 273, 282 (S.D.N.Y. 2008), a data breach case in which the court found plaintiffs had standing to pursue their negligence claim, but failed to allege damages where they had not alleged any "actual misuse of information." Like *Hammond*, the *Caudle* court did not appear to consider the economic loss rule applicable to plaintiffs' claims, and the case suggests that Plaintiffs here adequately allege a negligence claim.

The Seventh Circuit's Opinion suggests that Plaintiffs' allegations satisfy the proximate cause element of their negligence claim as well as the "fairly traceable" requirement of Article III's standing analysis. The panel concluded: "It is certainly plausible for pleading purposes that [Plaintiffs'] injuries are 'fairly traceable' to the data breach at Neiman Marcus." (Opinion at 15 (quoting *Target*, 66 F. Supp. 3d at 1159). And the *Target* opinion that the panel quoted directly supports the proposition that Plaintiffs' allegations satisfy the causation requirement for purposes of Defendant's motion under Rule 12(b)(6) as well as under 12(b)(1). The *Target* court held: "Plaintiffs' allegations plausibly allege that they suffered injuries that are 'fairly traceable' to Target's conduct. This is sufficient at this stage to plead standing. Should discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment on the issue." 66 F. Supp. 3d at 1159; *see also AvMed*, 693 F.3d at 1321 ("[T]he Complaint sufficiently alleges the causation element of negligence, negligence per se, breach of contract, breach of implied contract, breach of the implied covenant of good faith and fair dealing, and breach of fiduciary duty . . . . The Complaint similarly alleges facts sufficient to withstand a motion to dismiss on the restitution/unjust enrichment claim.").

As argued in Plaintiffs' original opposition, Defendant's contentions regarding causation again raise questions of fact inappropriate for decision on this motion to dismiss. Indeed, the Seventh Circuit recognized as much when it observed that Defendant's argument that all fraudulent charges are reimbursed by banks 100% of the time "reveals a material factual dispute." (Opinion at 7.) While Defendant appears now to back off its prior heavy reliance on banks' "zero liability" policies that the Seventh Circuit focused on, the reasoning is the same with respect to any other causation arguments Defendant may advance in place of those policies.

In its supplemental briefing, Defendant appears to be relying on an "intervening tortfeasor"

theory to attack causation, pointing to the hackers who perpetrated the data breach to absolve Defendant of liability for its own negligent security practices that allowed the hackers to succeed. (Supp. Br. at 18.) But Defendant does not even attempt to engage in the appropriate analysis for such an intervening-tortfeasor argument. "[I]n deciding whether a defendant's conduct was a material and substantial element in bringing about an injury, we ask whether, absent the defendant's conduct, that injury still would have occurred. . . . The relevant inquiry here is whether the injury is of a type that a reasonable person would see as a *likely result* of his or her conduct." *First Springfield Bank & Tr. v. Galman*, 720 N.E.2d 1068, 1073 (Ill. 1999) (citing *Lee v. Chi. Transit Auth.*, 605 N.E.2d 493, 503 (Ill. 1992) ("'[A] negligent act is a proximate cause of an injury if the injury is of a type which a reasonable man would see as a likely result of his conduct.'") (citation omitted)).

Defendant does not and cannot dispute that the data breach was a foreseeable result of its deficient security practices, which included turning off features that could have prevented the data breach altogether. Defendant does not really make an argument directed to the proximate cause element of Plaintiffs' negligence claim and, thus, the motion should be denied on this basis.

E. <u>Plaintiffs Properly Plead Unjust Enrichment (Count III)</u>

With respect to Plaintiffs' unjust enrichment claim, Defendant largely relies on the argument in its original motion, but again argues that the Seventh Circuit somehow "invalid[ated Plaintiffs'] Overpayment Theory." (Supp. Br. at 19; *see also id.* at 20 ("The only issue implicated by the panel's Opinion is plaintiffs' reliance on the Overpayment Theory.").) Again, the Seventh Circuit did not rule upon this issue, and indeed cited authority supporting this very theory in the data breach context. *See AvMed*, 693 F.3d at 1328 (finding plaintiffs sufficiently pled unjust enrichment claim in data breach case where they alleged "that AvMed cannot equitably retain their monthly insurance premiums—part of which were intended to pay for the administrative costs of

data security—because AvMed did not properly secure Plaintiffs' data . . .").

In addition, Defendant argues that *Nat'l Union Fire Ins. Co. v. DiMucci*, 34 N.E.3d 1023, 1042 (Ill. App. Ct. 2015), somehow does not stand for the proposition it obviously supports, namely that there is no longer any basis for "casting the [unjust enrichment] claim in terms of a 'duty' requirement" under Illinois law. Defendant cites earlier federal authority to the contrary, which cannot trump this on-point state authority on this issue of state law. This case underscores the argument Plaintiffs made in their original opposition (Part V. F.), that Illinois law is basically similar to that of California, requiring that: "To prevail on a claim for unjust enrichment, a plaintiff must prove that the defendant 'retained a benefit to the plaintiff's detriment, and that defendant's retention of the benefit violates fundamental principles of justice, equity, and good conscience.'" *Id.* at 1043 (quoting *HPI Health Care Servs., Inc. v. Mt. Vernon Hospital, Inc.*, 545 N.E.2d 672, 137 (Ill. 1989)). There no longer is any need for Plaintiffs' to allege an "independent basis which establishes a duty on the part of the defendant . . . ." *Lewis v. Lead Indus. Ass'n, Inc.*, 342 Ill. App. 3d 95, 105 (Ill. App. Ct. 2003). However, as argued in Plaintiffs' original opposition, Plaintiffs satisfied any such requirement by alleging Defendant had a duty to "implement and maintain reasonable security procedures" imposed on it by statute as well as under the terms of the implied contract between the parties, and that Defendant violated that duty. Cal. Civ. Code § 1798.81.5; *see also Sony*, 996 F. Supp. 2d at 966 ("[A] legal duty to safeguard a consumer's confidential information entrusted to a commercial entity . . . [is] well supported by both common sense and California and Massachusetts law.") (citing, *inter alia*, *Witriol v. LexisNexis Group*, C05-02392 MJJ, 2006 WL 4725713, at *8 (N.D. Cal. Feb. 10, 2006)).

For these and the reasons set forth in Plaintiffs' original opposition, Plaintiffs sufficiently state a claim for unjust enrichment.

F. Plaintiffs Properly Plead Invasion of Privacy Under California Law (Count V)

As argued in Plaintiffs' original opposition, Plaintiffs state a claim for invasion of privacy under California law. In its supplemental brief, Defendant misrepresents the Seventh Circuit's Opinion regarding the allegations supporting this claim. The Seventh Circuit's Opinion considered only standing under Article III, and with respect to Plaintiffs' allegations concerning their claim for invasion of privacy, the court reasoned that because no "***federal law*** recognizes such a property right," the panel "refrain[ed] from supporting standing" on this theory. (Opinion at 13.) Plaintiffs do not premise this claim on federal law, but on California law, which clearly recognizes a right to privacy, including in the California Constitution. *See* Cal. Const., Art. 1, § 1; *see also Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 806 (N.D. Cal. 2011) (quoting *KNB Enterprises v. Matthews*, 78 Cal. App. 4th 362, 366 (Cal. Ct. App. 2000)). As Plaintiffs have Article III standing, they are free to pursue these state law claims in this Court.

For these and all of the reasons set forth in Part V.G of the original opposition, Plaintiffs state a claim under California law.

IV. CONCLUSION

For the reasons stated herein, Defendant's motion to dismiss should be denied.

Dated: December 7, 2015

Respectfully submitted,

/s/ Tina Wolfson
Tina Wolfson
twolfson@ahdootwolfson.com
Robert Ahdoot
rahdoot@ahdootwolfson.com
Theodore W. Maya
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, California 90069
Tel: 310-474-9111

Fax: 310-474-8585

/s/ John A. Yanchunis
John A. Yanchunis
jyanchunis@forthepeople.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: 813-275-5272
Fax: 813-226-5402

/s/ Joseph J. Siprut
Joseph J. Siprut
jsiprut@siprut.com
SIPRUT PC
17 North State Street, Suite 1600
Chicago, Illinois 60602
Tel: 312-236-0000
Fax: 312-878-1342

CERTIFICATE OF SERVICE

The undersigned, an attorney, hereby certifies that a true and correct copy of the foregoing **Plaintiff's Response In Opposition To Neiman Marcus Group, LLC's Supplemental Brief In Support Of Its Motion To Dismiss Plaintiffs' First Amended Complaint** was filed this 7th day of December 2015 via the electronic filing system of the Northern District of Illinois, which will automatically serve all counsel of record.

/s/ Tina Wolfson